⑫ # EUROPEAN PATENT APPLICATION

㉜ Inventor : Francini, Joseph P.
18574 Greenridge Court
Castro Valley, California 94552 (US)
Inventor : Asbo, Einar L.
110 Reed Street
Mill Valley, California 94941 (US)

㉞ Representative : Jackson, David Spence
REDDIE & GROSE 16, Theobalds Road
London, WC1X 8PL (GB)

㉞ A system for validating the authenticity of a transaction employing electronic receipts.

㊗ A digitized code signal representative of the signature of the purchaser is generated at the point of sale by the transaction terminal (36). This code signal along with the parameters of the transaction are stored (52) electronically. In the event that the customer questions the transaction, the financial institution (26) associated with the merchant (34) can generate a hard copy receipt which includes the parameters of the transaction as well as a representation of the signature of the purchaser. This hard copy receipt is then sent to the customer for validating the transaction. This eliminates the need to generate, transfer and store hard copy receipts unless they are specifically requested. At sale, transaction parameters are entered into an electronic cash register (38). A module (40) displays transaction data on a CRT (42). The module (40) may have a slot (46) for reading a magnetic stripe transaction card (22). Signature is effected with a light pen (44).

EP 0 474 360 A2

ELECTRONIC
CASH
REGISTER
38

36

42

46

40

THE MARKET RESTAURANT
1855 D STREET
ANYTOWN, USA
SEPT. 27, 1989

SUBTOTAL $24.50
TAX
TIP   5.00

TOTAL $29.50

John L. Cardy

JOHN L. CARDY
VISA 4000 000 73101
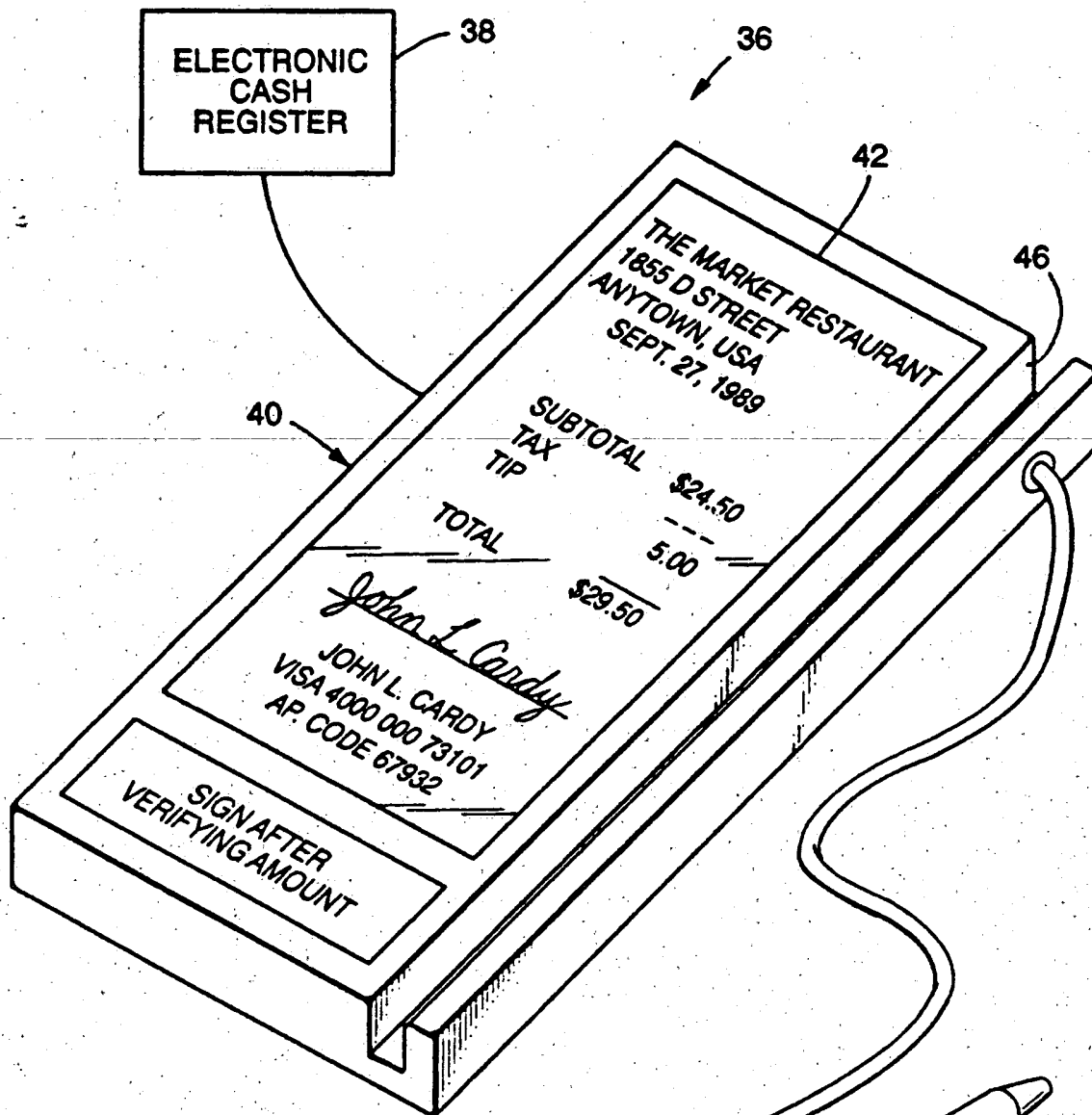AP. CODE 67932

SIGN AFTER
VERIFYING AMOUNT

FIG. 2

44

LIGHT PEN

Technical field

The subject invention relates to a system for authenticating transactions. The subject inv ntion is suitable for use with transaction card systems which heretofore have required hard copy receipts to authenticate transactions.

Background of the Invention

In today's environment, transaction cards are used as the preferred form of payment in a large number of transactions for the purchase of goods and services. There are different types of transaction or payment cards, such as credit and debit cards. In most cases, the customer presents the card at the point of purchase. The merchant will then take some steps to determine if the card if valid. If the merchant decides to accept the card, the transaction can be completed.

In most transactions involving a payment card, the purchaser is requested to provide a signature on a hard copy receipt. This receipt also includes various parameters identifying the transaction. These parameters typically include the account number of the card, expiration date, an identification of the merchant, the date, an approval code and the amount of the transaction.

The hard copy receipt is actually a composite of two to four essentially identical copies. After the customer has signed the receipt, he is usually given one of the copies. The customer saves this receipt for his records. One or more copies are retained by the merchant. Another copy of the receipt is sent to the financial institution associated with the merchant and responsible for generating the information that will ultimately result in a debit to the account of the customer.

At the present time, financial institutions generally save all the receipts from all transactions until payment is received. However, after the information from the receipts is used to bill the clients, they are not accessed again unless a dispute as to the authenticity of the transaction arises. More particularly, if a customer questions a bill for a particular transaction, he will contact the financial institution which issued his card. The latter institution will start an inquiry which includes the financial institution associated with the merchant identified on the customer's bill. The merchant's financial institution will then track down the receipt and prepare a copy for transmittal to the purchaser. Assuming the transaction was valid, the signature on the receipt is usually sufficient evidence to convince the customer that th purchase was made and that he is liable for the amount of the bill.

As can be appreciated, the need to store a very large volume of receipts in a manner that they can be accessed is a problem. This problem has been addressed in a number of ways. One approach has relied on the use of microfilm technology. In this approach, all of the receipts are microfilmed and catalogued to facilitate r tri val.

Another, more sophisticated approach is through the use of electronic image generation, storage and retrieval systems. Using these systems, the financial institution can generate a digital image of each of the receipts in much the same way as a facsimile machine converts an image to electronic impulses. These digital images can be catalogued and stored and regenerated as hard copies upon request to validate a transaction.

While the latter approaches alleviate the storage problem, they fail to address the more expensive and time consuming problem of actually handling the receipts. As noted above, a copy of every receipt must be transferred from the merchant to the associated financial institution. Thereafter, the financial institution must have human operators catalog and store the receipts, whether in hard copy, microfilm or electronic format.

One approach which has been suggested to eliminate the use of hard copy receipts is to require the user to supply a personal identification number (PIN), instead of a signature, at the time of the transaction. The requirement of supplying a PIN adds an additional level of security for the transaction. However, it does not provide a satisfactory solution to an inquiry by a purchaser. The response by the financial institution is limited to a statement to the customer that his PIN was used at the point of sale. No actual proof can be given to the customer which supports this statement. Moreover, even if proof could be given, a purchaser is much more willing to accept physical evidence of his signature as proof that he is liable for a transaction.

Therefore, it is an object of the subject invention to provide a system for authenticating a transaction that overcomes the problems of the prior art approaches.

It is another object of the subject invention to provide a system for authenticating transactions which eliminates the need to transfer and catalogue hard copy receipts.

It is a further object of the subject invention to provide a system for authenticating transactions which does not require transfer of a hard copy receipt, yet allows for the subsequent generation of such a receipt upon request.

It is still another object of the subject invention to provide a system for authenticating transactions which includes a terminal, or peripheral to a terminal, capable of generating a digitized code signal based on data uniquely identifying a purchaser.

It is still a further object of the subject invention to provide a system for authenticating transactions which includes a terminal capable of generating a

digitized code signal based on the signature of a purchaser.

It is still another object of the subj ct invention to provide a system for authenticating transactions which includes a terminal capable of generating a digitized code signal based on data uniquely identifying a purchaser and storing said code signal along with the parameters of the transaction.

It is still a further object of the subject invention to provide a system for authenticating transactions which includes a terminal capable of generating a digitized code signal based on data uniquely identifying a purchaser and storing said code signal along with the parameters of the transaction, with the data being used at a subsequent time to generate a hard copy receipt.

Summary of the Invention

In accordance with these and many other objects, the subject invention provides a method and system for validating the authenticity of a transaction. The system includes a terminal located at the point of sale for capturing the parameters of the transaction. In this respect, the terminal is like prior art terminals including electronic cash registers and other state of the art point of sale systems.

In accordance with the subject invention, the terminal is also provided with a means for electronically capturing data, supplied by the purchaser, and uniquely identifying that purchaser. In the preferred embodiment that data is a digital representation of a signature. There are a number of methods which can be used to generate a digital representation of a signature. For example, various digitizing pads and/or pens having pressure activated transducers have been used to record the digital signature information.

In the preferred embodiment of the subject invention, the digitized signature is created using a combination of a CRT and light pen. The latter combination has been used to record signatures in the prior art. (See, U.S. Patent No. 4,656,662, issued April 7, 1987). Although not clearly stated in the patent, it appears that the latter system was designed to generate a plurality of reference signatures for a customer base of a financial institution. These reference signatures could be accessed by the financial institution to identify a customer's signature, for example, when clearing a check. This approach would enable a financial institution to do away with signature cards.

In accordance with the subject invention, the digitized signature and the parameters of the transaction are stored in the terminal. All the data can th n be transmitt d from th terminal to the processor at the financial institution associated with the merchant (typically referred to as the acquirer). The acquirer will store this data until th payment for th transaction has been received. However, if the purchaser requests verification of the transaction, this data can be retrieved and a hard copy thereof can be generated. A variety of devices are availabl for converting the el ctronic data into a hard copy receipt. This hard copy receipt can then be supplied to the customer to validate the transaction and induce payment for the purchase.

As can be appreciated, the subject system allows for the same type of verification which is presently available but eliminates the need to create, catalogue and store physical, hard copy receipts. further objects and advantages will become apparent from the following detailed description, taken in conjunction with the drawings in which:

Brief Description of the Drawings:

Figure 1 is a schematic diagram of a typical transaction card network in which the subject invention can be implemented.

Figure 2 is a perspective view, partially in schematic, of a terminal for use in the system of the subject invention.

Detailed Description of the Preferred Embodiment

Turning to figure 1 there is illustrated a schematic diagram of a typical transaction card network 10. A more detailed description of this type of network is set forth in U.S. Patent No. 4,485,300, issued march 27, 1984, and incorporated herein by reference. Briefly, the network includes a plurality of financial institutions 20 that issue transaction cards 22 to customers. The network also includes a number of merchants 34 where the customer can purchase goods and services by using the payment card 22. Each merchant is associated with its own financial institution known as the acquirer 26.

The issuers and the acquirers are tied together into the network via a central processor 28 maintained by the network operator (ie. such as Visa or Mastercard). In a typical credit card transaction, the customer will present his card for a purchase. The merchant 34 will determine if the card is authentic through one of a number of approaches. For example, an authorization request can be generated and routed through the network to the issuer for approval. Additional information about authenticating cards can be found in U.S. Patent No. 4,734,564, issued March 29, 1988. (It should be noted that in some transactions, the issuer and the acquirer are the same financial institution. In this case, intervention by the network operator is unn cessary.)

If the card has b en auth nticated, the purchase can be completed. As noted above, the customer is typically asked to sign a hard copy receipt. At l ast one of these copies is eventually delivered to the acquirer. In some cases, the information on this

receipt is used by the acquirer to begin the billing process. In other cases, the receipt is merely catalogued and stored. In the latter case, information about the transaction will have been supplied to the acquir r from the merchant in an electronic format. There exists in the prior art a wide variety of merchant terminals which can capture the parameters of the transaction and periodically transmit them to the acquirer.

Once the acquirer has received the parameters of the transaction, they can be routed through the central processor 28 to the appropriate issuer. The issuer 20 then bills the cardholder.

If the cardholder disputes a bill on his statement, he will contact the issuer 20. The issuer will then initiate a request for information from the acquirer. The acquirer will then provide a hard copy of the receipt, with the cardholder's signature to confirm the transaction.

In accordance with the subject invention, the creation, storage and retrieval of the purchase receipt is substantially simplified. More particularly, the terminal at the merchant is provided with a means for creating a digitized code signal consisting of a representation of the signature of the cardholder. This code signal, along with the parameters of the transaction, is then transmitted electronically to the acquirer. The acquirer stores this data until an inquiry is initiated by the cardholder. If such an inquiry is made, the acquirer can then generate a hard copy receipt which is supplied to the cardholder to authenticate the transaction.

Figure 2 illustrates one type of terminal 36 which can be used to implement the subject invention. The terminal 36 can include a standard electronic cash register 38. This type of cash register has the capability of receiving inputs defining the date and amount of the transaction. This information can be stored in a digital fashion.

In accordance with the subject invention, a means is connected to the cash register 38 capable of creating a digitized version of the signature of the cardholder. As noted above, there are a number of devices available for converting the pen strokes of an individual into digital signals. For example, pressure pads and/or digitizing pens could be used.

In the preferred embodiment, the means is defined by a microprocessor driven module 40 including a CRT display 42 and a light pen 44. The module can also be provided with a means for reading the magnetic stripe on the transaction card (shown as a slot 46 in Figure 2).

In operation, the merchant can enter the transaction parameters into the cash register 38. The merchant will then swipe the magnetic stripe of the transaction card through slot 46 so that card identifying data can be read. This card identifying data can be transmitted through the network to obtain an authorization. The authorization can include a confirmation that the card has not been reported as lost or stolen.

Assuming that the transaction has been authorized, the parameters of the transaction will be displayed on the CRT display 42. As shown in figure 2, these parameters can include the merchant name, date of the transaction, transaction amount, cardholder's name, and transaction number. The customer is then given a chance to review the displayed information for accuracy. If the data is dorrect, the customer will then "sign" the display using the light pen 44.

As noted above, the use of the combination of a light pen and CRT display for digitizing handwritten data is well known and will not be described in detail. Briefly, in this type of device, the light pen includes a photodetector which is excited by the electron beam of the CRT. The current generated by the photodetector within the pen is correlated with the timing and position of the electron beam of the CRT to give positional information. The positional information is stored and supplied to the cash register 38. The unit can be programmed to display the signature as the user writes it on the CRT.

Once the user finishes entering his signature, the cash register can be used to generate a receipt, either with or without a facsimile of the signature. In this manner, the customer will have his own record of the transaction.

In accordance with the subject invention, no additional hard copy receipt needs to be generated at the time of purchase. The electronic digital data, which includes the transaction parameters and the signature information, can either be stored at the merchant location or transmitted to the acquirer. The acquirer can use this data to initiate the steps necessary to cause the issuer to bill the purchaser. In addition, the acquirer will store this information until the payment has been received.

As noted above, if a cardholder questions a billing entry on his statement, a request for confirmation will be sent by the issuer to the acquirer. At this point, the processor 50 operated by the acquirer will retrieve the data concerning the transaction from electronic storage 52 (Figure 1). The digital data can then be converted into human readable form, preferably, a hard copy receipt. This receipt will include all the transaction parameters including a representation of the customer's signature.

There are many devices 54 available for converting the stored digital data into hard copy receipts. This technology has been developed for various document storage and retrieval systems. This technology has also been used to digitize and store hard copy receipts and generate the receipts for later use.

Once the hard copy receipt has be n generat d, it can be sent to th customer to validate the transaction. Once the customer is presented with the rec ipt having his signature, most disputes can be resolved. As can be appreciated, the customer can b provided

with a confirming hard copy receipt even if a hard copy receipt was never generated at the point of sale. In this manner, the problems of transfer, cataloguing and storag of such receipts is liminated.

While the subject invention has been described with reference to a preferred embodiment, various changes and modifications could be made, by one skilled in the art, without varying from the scope and spirit of the subject invention as defined by the claims. For example, the identifying indicia need not be limited to the signature of the customer as any written code would suffice. In addition, the system could also be used to store and retrieve a PIN entry, providing proof to the customer that the valid PIN was entered. The human readable rendition of the receipt would not necessarily have to be a hard copy. For example, if the customer comes into a financial institution connected to the acquirer, the requested information could be electronically retrieved and used to generate a human readable image on a CRT screen where the customer is located. As long as the customer can review the information, the transaction can be validated.
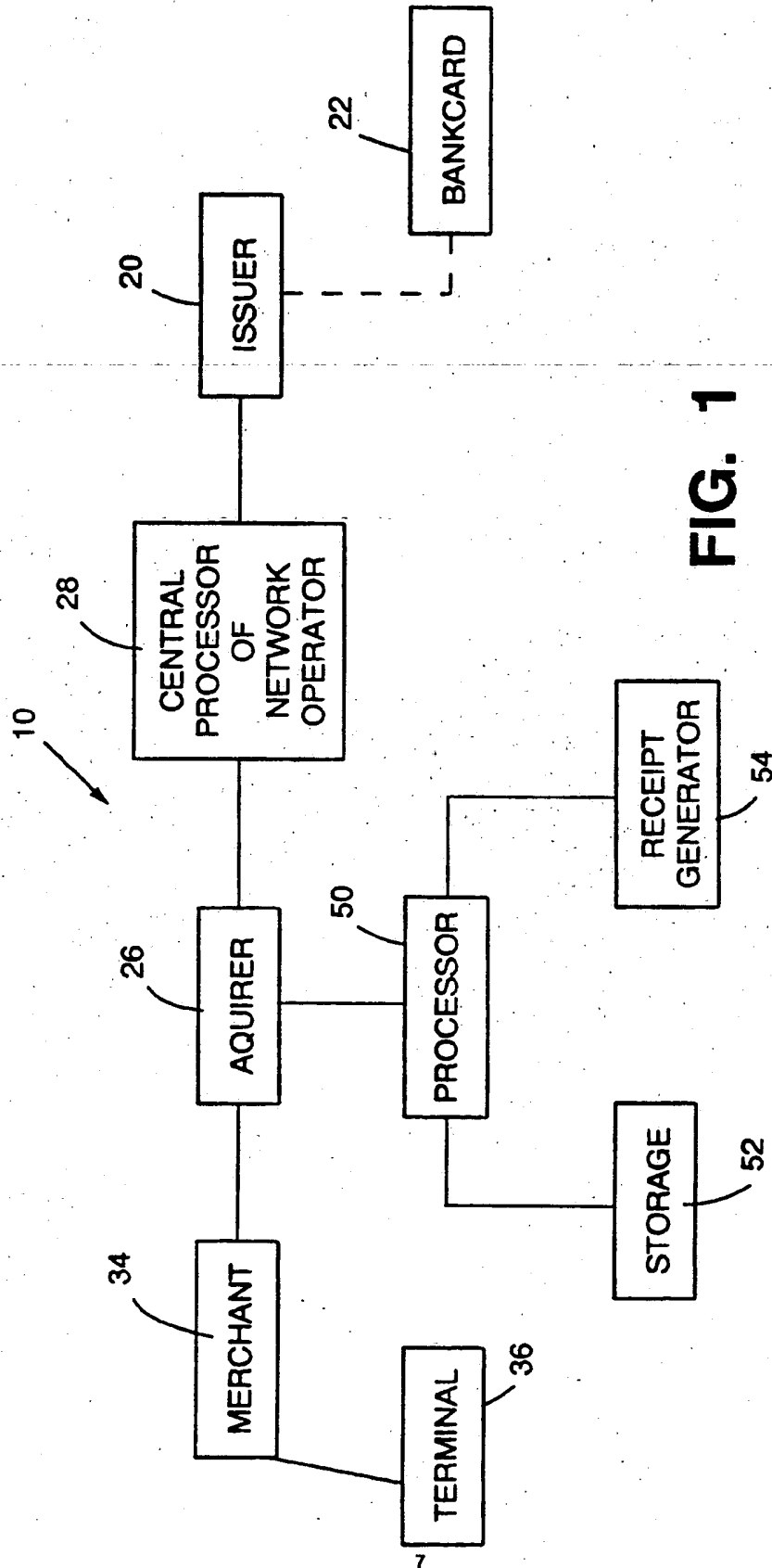
Claims

1. A method for validating the authenticity of a transaction comprising the steps of:

generating a digitized code signal at the time of the transaction, said code signal being based on data supplied by the purchaser and uniquely identifying that purchaser;

storing said digitized code signal along with the digitized parameters of the transaction; and

generating a receipt in human readable format, said receipt including the parameters of the transaction and a representation of the data uniquely identifying the purchaser to permit the authenticity of the transaction to be validated.

2. A method as recited in claim 1 further including the step of transmitting the stored digitized code signal along with the digitized parameters of the transaction to a central processor for storage until such time as a request to generate a receipt is made.

3. A method as recited in claim 1 wherein said data uniquely identifying the purchaser is a signature.

4. A method as recited in claim 1 wherein said r c ipt is a hard copy receipt.

5. A system for validating the authenticity of a transaction comprising:
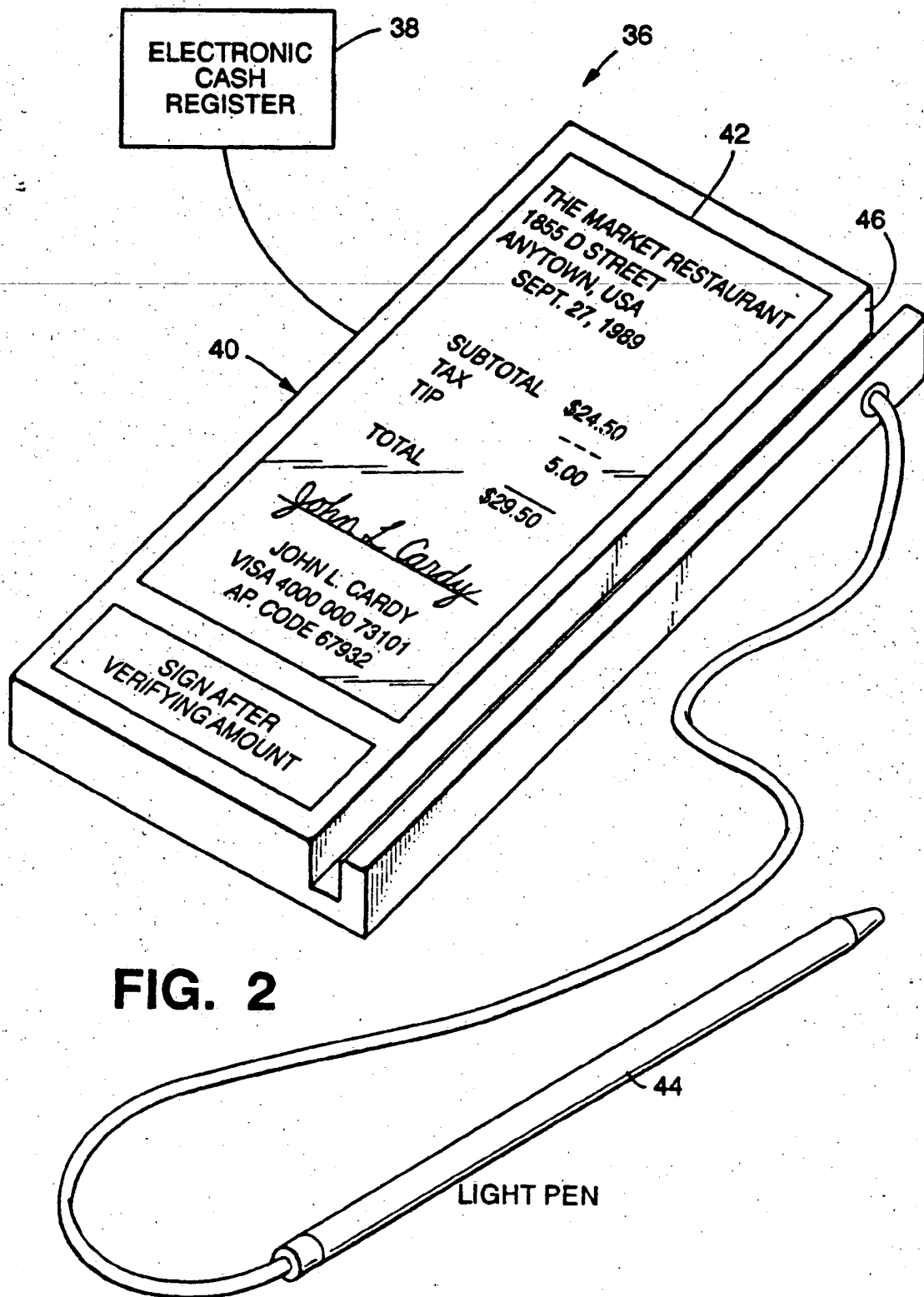
terminal means for recording the par-

ameters of the transaction, said terminal means also for recording a digitized code signal based on data suppli d by th purchaser and uniquely identifying that purchaser; and

means connectable to said terminal means for generating a receipt in human readable format, said receipt including the parameters of the transaction and a representation of the data uniquely identifying the purchaser to permit the authenticity of the transaction to be validated.

6. A system as recited in claim 5 wherein said data uniquely identifying the purchaser is a signature.

7. A system as recited in claim 5 wherein said receipt is a hard copy receipt.

8. A terminal for use in a system for validating the authenticity of a transaction comprising:

means for recording the parameters of the transaction; and

means for recording a digitized code signal based on data supplied by the purchaser and uniquely identifying that purchaser so that a receipt can be generated at a later time, said receipt being in human readable format and including the parameters of the transaction and a representation of the data uniquely identifying the purchaser to permit the authenticity of the transaction to be validated.

9. A terminal as recited in claim 8 wherein said terminal further includes a means for displaying the transaction parameters at the time of the transaction.

10. A terminal as recited in claim 8 wherein said data uniquely identifying the purchaser is a signature.

11. A terminal as recited in claim 8 wherein said means for recording the digitized code signals includes a CRT in combination with a light pen.

12. A terminal as recited in claim 8 wherein a human readable receipt is also generated at the time of the transaction.

13. A terminal as recited in claim 8 wherein said receipt is a hard copy receipt.

FIG. 1

FIG. 2